

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California
Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC.,
a Delaware corporation, INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation, and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

C. A. No. 04-1199 (SLR)

PUBLIC VERSION

**SRI INTERNATIONAL, INC.'S RESPONSE TO DEFENDANTS'
JOINT MOTION FOR SUMMARY JUDGMENT OF
INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103**

Dated: June 30, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. SUMMARY OF ARGUMENT	1
III. ARGUMENT	3
A. Legal Standards.....	3
B. The <i>EMERALD 1997</i> Reference Does Not Anticipate or Render Obvious the Claims of the Patents-in-Suit	5
1. The <i>EMERALD 1997</i> reference does not anticipate the claims of the '203 or the '615 patents	6
2. The claims of the '203 and '615 patents are not rendered obvious by a combination of <i>EMERALD 1997</i> and <i>Intrusive Activity 1991</i>	10
3. The <i>EMERALD 1997</i> reference does not Anticipate or Render obvious the claims of the '212 patent	14
C. The <i>Live Traffic</i> References Do Not Anticipate or Render Obvious the Claims of the Patents-in-Suit	17
1. The Symposium version of the <i>Live Traffic</i> paper is not prior art under § 102(a)	18
2. The HTML version of the <i>Live Traffic</i> paper is not prior art under § 102(b).....	19
D. The <i>JiNao Report</i> Does Not Anticipate the Claims of the Patents-in-Suit.....	21
1. The <i>JiNao Report</i> does not anticipate the hierarchical claims of the patents-in-suit	22
2. The <i>JiNao Report</i> does not anticipate the '338 claims	25
E. The Defendants' Failure to Address Secondary Considerations of Nonobviousness Precludes Any Summary Judgment of Invalidity Under § 103.....	30
IV. CONCLUSION.....	31

TABLE OF CONTENTS

	<u>Page</u>
<u>Cases</u>	
<i>Akamai Techs., Inc. v. Cable & Wireless Internet Services, Inc.</i> , 344 F.3d 1186 (Fed. Cir. 2003).....	4, 8
<i>Application of Saunders</i> , 444 F.2d 599 (C.C.P.A. 1971)	10, 11, 12
<i>Bruckelmyer v. Ground Heaters</i> , No. 05-1412, 2006 445 F.3d 1374 (Fed. Cir. 2006)	19
<i>Celotex Corp. v. Catrett</i> , 477 U.S. 317 (1986).....	3, 24
<i>Connell v. Sears Roebuck & Co.</i> , 722 F.2d 1542 (Fed. Cir. 1983).....	4
<i>Elan Pharma., Inc. v. Mayo Found. For Med. Educ. & Research</i> , 346 F.3d 1051 (Fed. Cir. 2003).....	4
<i>Freedman Seating Co. v. American Seating Co.</i> 420 F.3d 1350 (Fed. Cir. 2005).....	10
<i>General Electric Co. v. Nintendo Co.</i> , 179 F.3d 1350 (Fed.Cir.1999).....	14
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966).....	10
<i>In re Bayer</i> , 568 F.2d 1357 (C.C.P.A. 1978)	19, 21
<i>In re Cronyn</i> , 890 F.2d 1158 (Fed. Cir. 1989).....	19, 20, 21
<i>In re Hall</i> , 781 F.2d 897 (Fed. Cir. 1986).....	19
<i>In re Tenney</i> , 254 F.2d 619 (C.C.P.A. 1958)	20
<i>In re Wyer</i> , 655 F.2d 221 (C.C.P.A. 1981)	19

<i>Invitrogen Corp. v. Biocrest Mfg., L.P.</i> , 424 F.3d 1374 (Fed. Cir. 2005).....	4
<i>Matsushita Elec. Indus. Co. v. Zenith Radio Corp.</i> , 475 U.S. 574 (1986).....	3, 30
<i>Metabolite Labs., Inc. v. Lab. Corp. of America Holdings</i> , 370 F.3d 1354 (Fed. Cir. 2004).....	4, 6
<i>Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.</i> , 976 F.2d 1559 (Fed. Cir. 1992).....	4
<i>Monarch Knitting Mach. Corp. v. Sulzer Morat GMBH</i> , 139 F.3d 877 (Fed. Cir. 1998).....	5, 30
<i>Norian Corp. v. Stryker Corp.</i> , 363 F.3d 1321 (Fed. Cir. 2004).....	19
<i>Perricone v. Medicis Pharm. Corp.</i> , 432 F.3d 1368 (Fed. Cir. 2005).....	4
<i>Quad Envtl. Tech. Corp. v. Union Sanitary Dist.</i> , 946 F.2d 870 (Fed. Cir. 1991).....	5
<i>Rheox v. United Catalysts</i> , 1995 U.S. Dist. LEXIS 13054 (D.N.J. 1995)	11
<i>Rockwell Int'l Corp. v. The United States</i> , 147 F.3d 1358 (Fed Cir. 1998).....	5, 30
<i>Ruiz v. A.B. Chance Co.</i> , 234 F.3d 654 (Fed. Cir. 2000).....	5, 30
<i>Schumer v Laboratory Computer Sys., Inc.</i> , 308 F.3d 1304 (Fed. Cir. 2002).....	4
<i>Scimed Life Systems, Inc. v. Johnson & Johnson</i> , 225 F.Supp.2d 422 (D. Del. 2002).....	30
<i>Toro Co. v. Deere & Co.</i> , 355 F.3d 1313 (Fed. Cir. 2004).....	4, 7
<i>TypeRight Keyboard Corp. v. Microsoft Corp.</i> , 374 F.3d 1151 (Fed. Cir. 2004).....	19

Treatises

<i>Manual of Patent Examining Procedure,</i> 609.02.....	7
---	---

8

35 U.S.C § 103	4, 13
35 U.S.C. § 102.....	2, 18, 19, 20
35 U.S.C. § 282.....	4, 5
37 C.F.R. 1.53	7
37 C.F.R. 1.57	11, 12, 17
FED. R. CIV. P. 56.....	3, 24

I. INTRODUCTION

Forty pages of briefing, 106 footnotes, and 42 attachments — including 159 pages of microscopically-small claim charts and 83 pages of expert declaration — should have indicated to the Defendants’ counsel that they simply cannot meet the high burden to establish invalidity by clear and convincing evidence in the context of summary judgment. In addition to the many factual issues,¹ detailed below, that preclude entry of judgment in their favor, the Defendants are forced to rely on legal theories which themselves are not summary judgment candidates. First, their primary references were cited to and considered by the Patent Office. The Defendants cite no case granting summary judgment of invalidity in this situation, and SRI is aware of none. Second, the Defendants rely on “inherent anticipation,” a particularly fact-laden inquiry which, again, is a singularly inappropriate tool for achieving affirmative summary of invalidity. Not surprisingly, the Defendants can cite no case granting summary judgment of invalidity on this issue. Finally, while there are a few extraordinary cases where obviousness has been disposed of on summary judgment, the Defendants make no attempt to draw parallels between those cases and this one, and there are none.

II. SUMMARY OF ARGUMENT

This is a technically complicated, multi-patent, multi-defendant software case. While SRI believes certain *issues* can be disposed of on summary judgment, as discussed in its own motions, the entire case cannot be, let alone on the multiple, independent grounds presented in the Defendants’ many prolix motions.

Specific reasons this motion should be denied include:

1. *EMERALD 1997*, which was cited to and considered by the Patent Office, does not anticipate or render obvious any claims of the patents-in-suit, at least because it does

¹ The Defendants introduce twenty issues of relevance in this case under the heading “Established Facts.” Joint Invalidity Brief (D.I. 297) at 16-18. That heading is misleading in that only five of the enumerated issues — 1-2 and 4-6 — are undisputed by the parties. SRI contests issues 3 and 7-20.

not disclose analysis of the specific types of network traffic claimed and does not enable the claimed statistical detection methods. The Defendants have failed to carry the heavy burden of demonstrating that *EMERALD 1997* inherently anticipates the claims of the '203 and '615 patents. The Defendants' Exhibit W², in fact, makes the point that critical disclosure which specifically supports the asserted claims is absent from *EMERALD 1997*, which the inventors testified was an early, high-level description of an unfinished work-in-progress. Likewise, the Defendants have failed to show by clear and convincing evidence that one of ordinary skill in the art would have been motivated to combine *EMERALD 1997* and the *Intrusive Activity 1991* reference or that the combination would include all the elements of the claims, and accordingly, the Defendants are not entitled to summary judgment invalidating claims of the '203 and '615 patents on obviousness grounds.

2. The *Live Traffic* references do not anticipate or render obvious any claims of the patents-in-suit because neither is prior art. The symposium publication of the *Live Traffic* paper is not prior art under 35 U.S.C. § 102(a) because it did not describe the inventions of the patents-in-suit "before the invention thereof by the inventors." The Defendants do not even attempt to explain how a publication by the inventors themselves, less than one year prior to filing their patent application, can qualify as Section 102(a) prior art. Similarly, the HTML version of the *Live Traffic* paper is not prior art under 35 U.S.C. § 102(b) because, as substantial evidence ignored by the Defendants shows, it was not publicly available one year prior to the date the '338 patent was filed. Indeed, as SRI has

² Attached to the Declaration of Renee Dubord Brown in Support of Defendants' Joint Motion for Summary Judgment of Invalidity (Brown Declaration) (D.I. 301).

shown in its own summary judgment filing, SRI is entitled to summary judgment in its favor on this issue.

3. The *JiNao Report* does not anticipate the claims of the patents-in-suit. It does not anticipate the hierarchical claims because it does not disclose a hierarchical monitor that automatically receives and integrates reports of suspicious activity from a plurality of network monitors. It does not anticipate the network monitor limitations because its intrusion detection function is not based on an analysis of network traffic data. It does not anticipate the asserted '338 claims because it does not disclose at least the limitation of those claims that requires building long-term and short-term statistical profiles based on measures of network packets.

4. In addition, because all evidence must be viewed in the light most favorable to SRI, the Defendants' failure to even address SRI's evidence regarding secondary considerations of non-obviousness precludes altogether summary judgment of obviousness of the patents-in-suit.

III. ARGUMENT

A. Legal Standards

Summary judgment is appropriate when "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). The party that seeks summary judgment carries the initial burden of proving that there are no genuine issues of material fact. *Id.* at 322-4. Because the burden is on the moving party, the Court must view all evidence in the light most favorable to the nonmoving party, and draw all inferences in favor of the nonmoving party. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

An issued patent is presumed to be valid, 35 U.S.C. § 282 (2000), and thus a party attempting to demonstrate invalidity of an issued patent must do so by clear and convincing evidence. *Connell v. Sears Roebuck & Co.*, 722 F.2d 1542, 1549 (Fed. Cir. 1983). This same standard of proof also applies in the summary judgment context. *Invitrogen Corp. v. Biocrest Mfg., L.P.*, 424 F.3d 1374, 1378 (Fed. Cir. 2005). Accordingly, “[t]he burden of proving invalidity on summary judgment is high.” *Schumer v. Laboratory Computer Sys., Inc.*, 308 F.3d 1304, 1316 (Fed. Cir. 2002).

To anticipate a claim, a single prior art reference must disclose every limitation of that claim. Limitations may be disclosed expressly or inherently. *Perricone v. Medicis Pharm. Corp.*, 432 F.3d 1368, 1375-1376 (Fed. Cir. 2005); *Minn. Mining & Mfg. Co. v. Johnson & Johnson Orthopaedics, Inc.*, 976 F.2d 1559, 1565 (Fed. Cir. 1992). In order to serve as an anticipating reference, the reference must enable that which it is asserted to anticipate. *Elan Pharma., Inc. v. Mayo Found. For Med. Educ. & Research*, 346 F.3d 1051, 1054 (Fed. Cir. 2003).

A claim limitation will only be found to be inherently present when the prior art reference necessarily includes the limitation. *Akamai Techs., Inc. v. Cable & Wireless Internet Services, Inc.*, 344 F.3d 1186, 1192 (Fed. Cir. 2003). It is not sufficient that a limitation is merely probably or possibly present in the reference. *Id.* Thus, for inherent anticipation to be found, the prior art must sufficiently describe and enable at least one embodiment which necessarily includes the subject matter embraced by the particular claim limitation. *Toro Co. v. Deere & Co.*, 355 F.3d 1313, 1321 (Fed. Cir. 2004). A party attempting to prove patent invalidity by inherent anticipation bears a particularly “heavy burden” when the purported anticipatory prior art reference was before the Patent and Trademark Office during prosecution. *Metabolite Labs., Inc. v. Lab. Corp. of America Holdings*, 370 F.3d 1354, 1368 (Fed. Cir. 2004).

As with anticipation, “[w]hen the issue is patent invalidity due to obviousness, 35 U.S.C. § 103, the movant must overcome the statutory presumption of validity, 35 U.S.C.

§ 282 by proving obviousness by clear and convincing evidence based on undisputed facts.” *Quad Envtl. Tech. Corp. v. Union Sanitary Dist.*, 946 F.2d 870, 872 (Fed. Cir. 1991). In such cases, “when material facts are disputed, and testimonial, documentary, and expert evidence are needed for their resolution, summary adjudication is not indicated.” *Id.* In accordance with Federal Circuit case law, “secondary considerations, when present, must be considered in determining obviousness.” *Ruiz v. A.B. Chance Co.*, 234 F.3d 654, 667 (Fed. Cir. 2000). Thus, the rule that evidence must be viewed in a light favorable to the non-moving party includes, in the context of summary judgment of obviousness, evidence of secondary considerations of nonobviousness. *Rockwell Int’l Corp. v. The United States*, 147 F.3d 1358, 1366 (Fed Cir. 1998). The existence of material issues of fact concerning such secondary considerations will preclude summary judgment of obviousness. *Id.*; *Monarch Knitting Mach. Corp. v. Sulzer Morat GMBH*, 139 F.3d 877, 886 (Fed. Cir. 1998).

The Defendants have failed to meet the heavy burden required to entitle them to summary judgment as to anticipation of the patents-in-suit here. Indeed, for reasons summarized below and set out in more detail in SRI’s own motions (D.I. 277, 271), SRI is entitled to judgment as a matter of law that the EMERALD 1997 and Live Traffic references do not anticipate any asserted claim. Further, the Defendants have not only failed to demonstrate that no issues of material fact exist as to obviousness, they have failed to even address numerous secondary considerations of nonobviousness. For these reasons, the Defendants’ request for summary judgment relating to obviousness must also be denied.

B. The EMERALD 1997 Reference Does Not Anticipate or Render Obvious the Claims of the Patents-in-Suit

*EMERALD 1997*³ is an early overview paper written by Philip Porras, one of the inventors of the patents-in-suit, shortly after he joined SRI. The paper describes a

³ Attached as Ex. E to the Brown Declaration.

proposed research program for developing a practicable, scalable architecture for identifying intrusions in large-scale enterprise networks, including potential solutions that SRI intended to pursue. [Porras Decl. ¶ 5]. Specifically, in *EMERALD 1997*, Mr. Porras identified numerous generic data sources that he viewed as potentially useful in tackling the intrusion detection problems outlined in the paper. The research proposed in *EMERALD 1997* eventually led to the conception and reduction to practice of the claimed inventions.

1. The *EMERALD 1997* reference does not anticipate the claims of the '203 or the '615 patents

The Defendants' own expert admits that the *EMERALD 1997* reference makes no explicit reference to any of the types of network traffic data recited in the Markush groups of the claims of the '615 and '203 patents. [Avolio Decl.⁴ ¶ 59]. The Defendants rely solely on an inherent anticipation argument. As noted above, the party attempting to prove patent invalidity by inherent anticipation bears a "heavy burden," especially when, as in this case, the prior art was before the Patent and Trademark Office during prosecution. *Metabolite Labs.*, 370 F.3d at 1368.

Contrary to Defendants' assertion, the *EMERALD 1997* reference was before the examiner during prosecution of all four patents-in-suit, including the '615 and the '203 patents. *EMERALD 1997* was cited as a reference directly on the face of the '338, '212, and '615 patents. Because the '203 patent resulted from a continuation of the application which resulted in the '338 patent, the applicant was not required to re-submit references submitted in the parent. Under the Manual of Patent Examining Procedure, the examiner is *required* to consider references submitted in a parent application when reviewing a

⁴ The Declaration of Mr. Avolio is attached as Ex. X to the Brown Declaration.

continuation application.⁵ *Manual of Patent Examining Procedure*, 609.02(A)(2). Thus, although not listed on the face of the '203 patent, the *EMERALD 1997* reference is presumed to have been considered during prosecution of all four of the patents-in-suit, including both the '615 and the '203. The Defendants thus are subject to a particularly heavy burden of proof in demonstrating inherent anticipation of either patent based on the cited *EMERALD 1997* reference.

For inherent anticipation to be found, the prior art must sufficiently describe and enable at least one embodiment which necessarily includes the subject matter embraced by the particular claim limitation. *Toro Co.*, 355 F.3d at 1321. Thus, to prevail on their summary judgment motion, the Defendants must prove by clear and convincing evidence that a person of ordinary skill in the art at the time of filing, attempting to design a network intrusion detection method using only *EMERALD 1997* as a guide, would necessarily construct a system which analyzes at least one type of network traffic data required by the Markush groups of the '615 and '203 patents. The Defendants' arguments fall far short of meeting this burden. Instead, they strain to equate one possible outcome with the required necessarily present claim limitations.

As explained in detail in SRI's own motion seeking judgment that *EMERALD 1997* does not, as a matter of law, inherently anticipate, The Defendants' argument is based on an untenable chain of inference that, even if followed, cannot result in a finding of inherent anticipation. The twisted path starts with the *EMERALD 1997* reference

⁵ "The examiner will consider information which has been considered by the Office in a parent application when examining (A) a continuation application filed under 37 C.F.R. 1.53(b) ** (B) a divisional application filed under 37 C.F.R. 1.53(b) ** or (C) a continuation-in-part application filed under 37 C.F.R. 1.53(b). A listing of the information need not be resubmitted in the continuing application unless the applicant desires the information to be printed on the patent." Ex. I, MPEP, 609.02(A)(2) (emphasis added).

suggesting monitoring a target specific event stream, which *may be* derived from a variety of sources including “application logs.” The Defendants argue that “application log” *could* include firewall logs. They then argue that firewalls allegedly must be configured to monitor network connection requests and denials, which are two of the network data types claimed in the ’203 and ’615 patents. Finally, they state that it was “standard practice” in 1997 for firewalls to monitor network packet data volume, another claimed data type. From this chain of inference, The Defendants ultimately conclude that monitoring of these three data types (network connection requests, network connection denials, and network packet data volume) is inherently disclosed in the *EMERALD 1997* reference.

The Defendants’ argument fails because it at best demonstrates that a person of ordinary skill, using the *EMERALD 1997* article as a guide, might *possibly* construct a network intrusion detection system which monitors a data type included in the Markush groups of the ’203 and ’615 patents. To inherently disclose a limitation, however, it is not enough that a reference possibly disclose a claim element — it must *necessarily* disclose it. *Akamai*, 344 F.3d at 1192 (Fed. Cir. 2003).

First, disclosure in *EMERALD 1997* of monitoring an application log would not necessarily lead a person of ordinary skill even to the first inference, *i.e.*, analyzing specifically firewall logs. See SRI’s Opening Brief in Support of Its Motion for Partial Summary Judgment of No Anticipation by the *EMERALD 1997* Publication (D.I. No. 277) at 7. Instead, as even the Defendants’ expert admits, “activity log” and “application log” are general terms, which may include firewall logs, but can also refer to logs of other types of activity and applications. [Ex. A at 64:12-25 and 65:1-2; Brown Decl, Ex. X, ¶

50]. Thus, the decision to implement the *EMERALD 1997* system using a firewall log rather than some other type of application log is a design choice, not an inherent feature disclosed in the reference.

Second, it does not follow that a firewall log, even if analyzed, would necessarily include the particular data types required by the patents-in-suit. As Mr. Avolio testified during his deposition,

REDACTED

[Ex. A at 42:5-14, 42:23-25, 43:3-4], and furthermore

REDACTED

[Ex. A at 71:23-25, 72:1-3]. Thus, even if a person of ordinary skill were to somehow read into the *EMERALD 1997* disclosure the *possibility* of logging one of the data types in the patent claims at issue, the decision to do so would merely represent yet another design choice, and not an inherent disclosure.

Given the many design choices identified by The Defendants' own experts, the path from the disclosure in *EMERALD 1997* to the creation of a system that selectively analyzes the particular types of network traffic data claimed in the '615 and '203 patents is neither direct nor inevitable. As a consequence, *EMERALD 1997* cannot inherently anticipate these claims. The Defendants, therefore, are not entitled to summary judgment on the issue of anticipation. On the contrary, SRI is entitled to summary judgment on its motion for summary judgment that the '338, '203, and '615 patent are not anticipated by the *EMERALD 1997* reference. [See SRI's Opening Brief in Support of Its Motion for Partial Summary Judgment of No Anticipation by the *EMERALD 1997* Publication (D.I. No. 277) at 14].

2. The claims of the '203 and '615 patents are not rendered obvious by a combination of *EMERALD 1997* and *Intrusive Activity 1991*

The asserted combination of *EMERALD 1997* and *Intrusive Activity 1991*⁶ cannot render any of the asserted claims obvious because there is no motivation to combine the references and, even if combined, the limitations of the claims are not present in the combination.

Obviousness is a question of law premised on underlying findings of fact. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966). Therefore where, as in this case, the non-moving party presents evidence showing that genuine issues of material fact remain as to the underlying factual issues relating to obviousness, the court should not grant summary judgment of invalidity. *Freedman Seating Co. v. American Seating Co.* 420 F.3d 1350, 1352 (Fed. Cir. 2005).

First, though the Defendants acknowledge their burden to show a motivation to combine, they have failed to do so by clear and convincing evidence. The Defendants claim that because the *EMERALD 1997* article cites the *Intrusive Activity 1991* reference, this constitutes an express motivation to combine the teachings of these two references. As authority for this argument, the Defendants cite *Application of Saunders*, 444 F.2d 599, 601 (C.C.P.A. 1971). But *Saunders* does not stand for the rule proposed by the Defendants.

Unlike this case, the *Saunders* case was an appeal from a USPTO decision which held that the applicant's claims were obvious in light of a primary reference which cited to a secondary reference. Both the cited references in *Saunders*, however, were issued U.S. patents. Certain relevant portions of the secondary reference had been incorporated

by reference during prosecution, which resulted in the issuance of the primary reference. Incorporation by reference in a patent application is governed by 37 C.F.R. 1.57, which allows incorporation **only for material contained in another U.S. patent or published patent application**. 37 C.F.R. 1.57(c) (“essential material” may be incorporated by reference, but only by way of an incorporation by reference to a U.S. patent or U.S. patent application publication . . .) (emphasis added).

Thus, the C.C.P.A in *Saunders* merely ruled that where a *portion* of a (secondary) U.S. patent is incorporated by reference into the disclosure of another (primary) U.S. patent, it would be obvious for a person of ordinary skill to combine the primary patent reference with other, *non-incorporated portions* of the secondary patent reference. *Application of Saunders*, 444 F.2d at 603 (“it would not have been necessary for one skilled in the art to have gone any further than another part of [the secondary patent reference]”). *Saunders* does not stand for the general proposition that a mere citation to, rather than an express incorporation of, one **non-patent** reference within another **non-patent** reference constitutes an express motivation to combine the two.⁷ Incorporation by reference applies to patents, as expressly provided under 37 C.F.R. 1.57. Patents are required to be enabling, and enablement may be achieved by incorporating other patents by reference. This same standards do not apply to technical papers. A non-patent

⁶ Attached as Ex. F to the Brown Declaration.

⁷ The Defendants’ also cite another case, *Rheox v. United Catalysts*, 1995 U.S. Dist. LEXIS 13054 (D.N.J. 1995), for the proposition that an internally cited reference may satisfy anticipation as well as obviousness. [Joint Invalidity Brief at 31, n.69]. However, *Rheox* also involved a U.S. patent incorporated by reference into the disclosure of another U.S. patent. Because the entire secondary reference was incorporated, the court held that the disclosure of both patents could be considered to be within “the four corners” of the primary patent. *Id.* at 12-13. Thus all the limitations of the patent-in-suit were found within the four corners of a *single reference*, and the *Rheox* court could find anticipation. Because both of the

reference may refer to another non-patent reference for any reason — there is no presumption that reference is made for purposes of enablement, and thus the same motivation to combine that may be presumed when one patent incorporates another by reference patent does not apply when one non-patent reference simply cites to another non-patent reference. Moreover, there is no comparable regulatory provision that provides for incorporation by reference in technical papers or other non-patent references.

Furthermore, the patent disclosure incorporated in the primary reference cited in *Saunders* was “essential material.”⁸ *Application of Saunders*, 444 F.2d at 601. In order to practice the invention claimed in the primary patent, a person of ordinary skill would thus have been *required* to consult the secondary patent reference. In this case, the primary reference (*EMERALD 1997*) makes only a one line mention, buried in a subsection on related work, to the secondary reference (*Intrusive Activity 1991*). [Brown Decl. Ex. E at 364]. A person of ordinary skill attempting to practice the disclosure of *EMERALD 1997* would not be required to consult the *Intrusive Activity 1991* article. In fact, such a person would be highly unlikely to consult the *Intrusive Activity* reference, since there would be no motivation to consult such an outdated technical article in a rapidly evolving field such as network security.

Second, even if a person of ordinary skill were somehow motivated to combine these disparate references, she would not find in that combination all the limitations of the claims of the '203 and '615 patents. [Ex. B ¶ 40]. It should be noted that among the Defendants' numerous experts, Mr. Heberlein alone finds the patent claims to be obvious

references cited by the Defendants here are technical articles, and not U.S. patents, and because here there is no incorporation by reference, *Rheox* is inapposite.

⁸ “Essential material” is material necessary to provide an enabling disclosure in a patent. 37 C.F.R. § 1.57(c)(1).

in light of the combination of *EMERALD 1997* and *Intrusive Activity 1991*. [Ex. B ¶ 38]. And Mr. Heberlein apparently cites the *Intrusive Activity* reference only for its disclosure of NSM, a reference which describes monitoring a local area networks, not enterprise networks, which are the subject of the SRI patents. *Id.* Further, NSM monitored only established connections between hosts. Because NSM only monitored *established connections*, it did not disclose monitoring network connection requests and denials. [Ex. B ¶ 38].

To get around this problem, the Defendants claim that *Intrusive Activity 1991* itself discloses monitoring of network connection requests and denials. The Defendants point to the following statement in the reference: “For example, network connections are created and destroyed continuously.” [Brown Decl. Ex. G at 365]. This statement does not disclose the monitoring, for network security purposes, of any of the data types required by the Markush claims of the ’203 and ’615 patents. The statement merely lists one of the difficulties to be addressed in designing a meta-language for operation in a broadcast LAN network security environment. *Id.* Rather than conducting a legitimate technical analysis, the Defendants merely attempt to find a few shreds of text which sound vaguely similar to the detailed disclosure of SRI’s patents. They then proceed to state (without any cited authority) that: “One of ordinary skill would have understood this disclosure of analyzing the creation and destruction of network connections to disclose monitoring “network connection requests” and “network connection denials.” This unsupported, conclusory attorney argument is simply insufficient to meet the Defendants’ burden of presenting clear and convincing evidence that the ’203 and ’615 patents are obvious under 35 U.S.C. § 103 in light of the cited references and Dr. Kesidis’ opinion

that these references, alone or in combination, do not invalidate the asserted claims. *See* Kesidis Rebuttal Rpt. at ¶¶ 38-40, 55. Further, as discussed more fully below, the Defendants' failure to even address secondary considerations of non-obviousness also precludes summary judgment of obviousness.

Overall, the Defendants face the same problem in both their anticipation and obviousness arguments. Neither *EMERALD 1997* nor *Intrusive Activity 1991*, alone or in combination, provides a person of ordinary skill with any guidance whatsoever as to what types of network data traffic to monitor in an enterprise network. Such guidance is found only in the disclosure and claims of SRI's patents. Without the impermissible guidance of hindsight, it would not have been obvious to one of ordinary skill in the art to select the specific types of traffic enumerated in the claimed inventions.⁹

3. The *EMERALD 1997* reference does not anticipate or render obvious the claims of the '212 patent

To anticipate a claim, a prior art reference must disclose every element of the challenged claim and **enable** one skilled in the art to make the anticipating subject matter. *General Electric Co. v. Nintendo Co.*, 179 F.3d 1350, 1356-57 (Fed.Cir.1999). The *EMERALD 1997* reference cannot anticipate claim 1 of the '212 patent, because it does not provide an **enabling** disclosure of the claimed invention. [Ex. B ¶ 24]. The Defendants argue that *EMERALD 1997* must be enabling, because of an alleged "striking similarity" between the reference and the patent specification. But as has been authoritatively made clear in the expert report of Dr. Kesidis [Ex. B ¶¶ 24-37], the alleged similarity between *EMERALD 1997* and the '212 patent is superficial at best.

⁹ Ex. B ¶ 35.

EMERALD 1997 described a proposal to attempt to adapt the earlier host-based NIDES approach to the problem of network anomaly detection. [Ex. B ¶ 24]. The problems inherent in attempting to scale-up the earlier host-based work to function in a large scale enterprise network were far from trivial. [Porras Decl. at ¶¶5-6]. As Dr. Kesidis states in his report:

REDACTED

[Ex. B ¶ 24].

The Defendants further assert that Mr. Valdes, a named inventor of the '212 patent, admitted that the *EMERALD 1997* reference disclosed the claimed invention of claim 1 of the '212 patent. The referenced portion of Mr. Valdes' deposition transcript does not support this assertion, and is taken out of context. Deposing counsel (Ms. Brown) begins the referenced line of questioning by attempting to get Mr. Valdes to admit that the claims of the '203 and '212 patents differ, in that the '212 discloses utilizing a statistical detection method where the '203 does not:

Q: Do you see the only difference is the '212 Claim 1 instead mentions utilizing - - utilizes a statistical detection method?¹⁰

Mr. Valdes, who is not trained in patent law and had not recently read the patents, did not understand the question and could not answer it. After several objections by SRI's

¹⁰ Ex. C at 461:19-21.

counsel, Ms. Brown is asked to repeat the question. Rather than repeating her question, however, she instead asks a different question altogether:

Q: Are there any other differences between those two claims?¹¹

Then, after some further questioning regarding the meaning of “enterprise network,” Ms. Brown changes direction again and asks the following:

Q: So what limitation or what portion or phrase, if you prefer, in ’212 Claim 1 is not disclosed in this publication?¹²

Mr. Valdes responds to this question as follows:

REDACTED

And finally:

REDACTED

This statement is merely an acknowledgment by the inventor that the claim language refers to the three elements identified immediately prior: *i.e.* – monitoring, enterprise network, and plurality. The statement does not make any reference to the key element of the ’212 claims – *statistical* detection of suspicious network activity. Therefore no reasonable interpretation of the transcript can be read as a statement by the inventor that the *EMERALD 1997* reference discloses all the elements of the ’212 patent claims.¹⁵

¹¹ Ex. C at 464:8-9 (emphasis added).

¹² Ex. C at 466:12-14.

¹³ Ex. C at 466:17-22 (emphasis added).

¹⁴ Ex. C at 467:3-5 (emphasis added).

¹⁵ This is especially true where the inventors, who are not trained in claim construction or legal analysis, were (over objection) subjected to hour after hour of semantically twisted word play on legal conclusions such as what the patent claims required and whether prior art references which the inventors had not even read met the claim language.

The Defendants further claim that it would have been obvious to combine *EMERALD 1997* with another internally cited reference, *NIDES 1994*. Apparently relying on the same flawed analysis of case law they use elsewhere, the Defendants cite *Saunders* for the proposition that there is always a motivation to combine a reference with another internally cited reference. However, as explained previously, the case does not stand for the general rule proposed by the Defendants. Because the references cited in the instant case (*EMERALD 1997* and *NIDES 1994*¹⁶) are technical articles, not U.S. patents, and because there is no express incorporation by reference here, *Saunders* is inapposite. As discussed above, while incorporation by reference of one patent into another is permitted under 37 C.F.R. 1.57, there is no comparable provision that applies to non-patent references. In fact, because the *NIDES 1994* reference is concerned with network security monitoring in *host-based systems*, a person of ordinary skill would not be motivated to combine this disparate reference when attempting to practice the *enterprise network system* disclosed in *EMERALD 1997*. [Ex. B ¶ 40]. And for the same reasons discussed above, the combination of these references, even if made, would not have enabled one of ordinary skill in the art to adapt the teachings of *NIDES* to the problem of enterprise network monitoring; this was a task that required significant research and experimentation even for the inventors themselves. [Ex. B ¶ 24].

C. The *Live Traffic* References Do Not Anticipate or Render Obvious the Claims of the Patents-in-Suit

Mr. Porras and Mr. Valdes, the inventors of the patents-in-suit, authored a paper entitled *Live Traffic Analysis of TCP/IP Gateways*, which discussed various aspects of the technology described in the patents-in-suit. Two versions of the *Live Traffic* paper

¹⁶ Attached as Ex. G to Brown Declaration.

are at issue. The final version of the paper — the “Symposium version” — was published in the Internet Society’s Networks and Distributed Systems Security Symposium proceedings in March 1998, less than one year before the filing date of the ’338 patent. The Defendants allege that, as part of the process for submitting the *Live Traffic* paper for publication in the symposium, Mr. Porras posted an earlier draft of the paper — the “HTML version” — on an FTP site and on the SRI web site, where it could be accessed by the symposium committee. The Defendants assert that this posting was a “publication” under section 102(b). The Defendants also assert, with no explanation, that the Symposium version of the paper constitutes prior art under 35 U.S.C. §102(a).

1. The Symposium version of the *Live Traffic* paper is not prior art under § 102(a)

Under 35 U.S.C. § 102(a), “a person shall be entitled to a patent unless the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent.” The Defendants make the peculiar argument that the symposium version of the *Live Traffic* paper is an anticipatory prior art reference that invalidates the claims under § 102(a). As noted above, the authors of the *Live Traffic* paper are the inventors. Therefore, the Defendants’ argument is that the symposium version of the *Live Traffic* paper is a publication by the inventors, describing the invention to others, before it was invented by the inventors. This argument makes no sense, as it would have been impossible for the inventors to have described their invention prior to their having invented it.¹⁷

¹⁷ Symantec’s patent law expert Stephen Kunin admitted that there was no basis under which the Symposium version of the *Live Traffic* paper would qualify as § 102 prior art. [Ex. D at 109:13-14].

2. The HTML version of the *Live Traffic* paper is not prior art under § 102(b)

The Defendants next contend that the HTML version of the *Live Traffic* paper is prior art under Section 102(b) because Mr. Porras allegedly posted it on an FTP site and the SRI website. The sum total of the Defendants' printed publication analysis, however, is a single paragraph on page 35 of their Joint Invalidity Brief that does not address the critical question: what is required for a document to be deemed "publicly accessible"?

SRI answered that question in its own motion addressed to this issue. The *Live Traffic* paper is not a printed publication and SRI is entitled to judgment as a matter of law to that effect. A document is a "printed publication" within the meaning of Section 102(b) "upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it and recognize and comprehend therefrom the essentials of the claimed invention without need of further research or experimentation." *Bruckelmyer v. Ground Heaters*, No. 05-1412, 2006 445 F.3d 1374, 1378 (Fed. Cir. 2006) (citing *In re Wyer*, 655 F.2d 221, 226 (C.C.P.A. 1981)). When claiming anticipation by a printed publication under Section 102(b), "[t]he party seeking to invalidate patent claims must do so by clear and convincing evidence." *TypeRight Keyboard Corp. v. Microsoft Corp.*, 374 F.3d 1151 (Fed. Cir. 2004) (citing *Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1326 (Fed. Cir. 2004)).

"Public accessibility" has been called the touchstone in determining whether a reference constitutes a 'printed publication' bar under 35 U.S.C. § 102(b)." *In re Hall*, 781 F.2d 897, 898-99 (Fed. Cir. 1986). "Access involves such factual inquiries as classification and indexing." *Wyer*, 655 F.2d at 226; *In re Cronyn*, 890 F.2d 1158, 1159 (Fed. Cir. 1989); *Hall*, 781 F.2d at 898; *In re Bayer*, 568 F.2d 1357, 1362 (C.C.P.A. 1978). Outside of general indices, in order to satisfy this requirement, the reference must be available by "customary research aids." *Bayer*, 568 F.2d at 1361. If the document

“could have been located ...only by one having been informed of its existence ..., and not by means of the customary research aids available,” the probability of public knowledge of the contents of the document is “virtually nil” and the reference does not constitute a printed publication. *Bayer*, 568 F.2d at 1362 (citing *In re Tenney*, 254 F.2d 619, 626 (C.C.P.A. 1958)).

Since the Defendants do not address any of the relevant factors regarding public accessibility, their motion should be denied on that basis alone. In fact, as detailed in SRI’s own motion, the evidence requires that judgment be entered against the Defendants on the question of the public accessibility of (and thus the question of anticipation by) the *Live Traffic* paper. See SRI’s Opening Brief in Support of its Motion for Partial Summary Judgment that the Live Traffic Article is not a Section 102(b) Printed Publication. SRI’s arguments in that brief are fully applicable here, and SRI respectfully incorporates them by reference.

The Defendants raise only one issue that was not addressed in SRI’s opening *Live Traffic* brief — the Defendants point to an SRI presentation in which Mr. Porras listed four web addresses on the FTP site as alleged proof that Mr. Porras intended to inform the DARPA community of the existence of papers posted on that site. [Ex. E at SRI105589]. Because the Defendants cite no case law whatsoever on this issue, it is unclear exactly why they believe Mr. Porras’ presentation, or his intent to inform the DARPA community of the existence of his papers in general, is significant. The specific article in question is not identified or addressed in the presentation. Presumably, the Defendants mean to suggest that the listing of four web addresses constituted an index. Yet even to the extent this exhibit from a presentation can be characterized as an index at all, it is not meaningful, as required by *Cronyn*, 890 F.2d at 1159, 1161.

The links to which the Defendants refer bear no discernable relationship to either the author or the nature of the specific subject matter concerned

REDACTED

[Ex. E at SRI105589]. Like the index found not to be meaningful in *Cronyn*, the list of FTP addresses is not meaningful because it does not identify the technical subject matter of the linked articles. Just like the theses in *Bayer* and in *Cronyn*, the FTP posting of the draft submission of the *Live Traffic* paper could not have been located by one of ordinary skill using customary research aids and reasonable diligence, even in view of Mr. Porras' presentation (which, again, does not mention the article), and therefore it was not publicly accessible.

D. The *JiNao Report* Does Not Anticipate the Claims of the Patents-in-Suit

The only prior art relied upon by the Defendants in the present motion that was not the work of SRI, relates to something called the "JiNao" project. Beginning in 1996, DARPA funded a three-year project aimed at designing and developing an intrusion detection system intended to prevent intruders from attacking specific types of network devices, such as network routers and switches. The project, called JiNao, was a joint collaboration between MCNC and North Carolina State University. The JiNao system, however, in part built on work previously done at SRI, with assistance from SRI researchers.¹⁸ A technical report on this work, entitled "Architecture Design of a Scalable Intrusion Detection System for the Emerging Network Infrastructure," was prepared by Y. Frank Jou in April 1997. That report is referred to as the *JiNao Report*.

¹⁸ Ex. F at 2; Ex. G at 27:21-28:20, 30:5-31:19, 40:1-41:12, 45:13-47:9.

1. The *JiNao Report* does not anticipate the hierarchical claims of the patents-in-suit

The *JiNao Report* does not anticipate any of the asserted claims of the '203, '615 or '212 patents because it fails to disclose at least two elements of the independent claims. First, it fails to disclose a hierarchical monitor that automatically receives and integrates reports of suspicious activity. [Ex. B ¶ 104]. Second, because JiNao teaches basing intrusion analysis on audit logs generated by a router, it fails to disclose a network monitor that detects suspicious activity based on an analysis of network traffic data. [Ex. B ¶¶ 101-103]. The Defendants' motion ignores this latter defect of the JiNao reference entirely.

The Defendants contend in the present motion that the hierarchical claims of the '203, '212, and '615 patents are invalid as anticipated by the *JiNao Report*. In support of this contention, the Defendants rely primarily on a diagram, Figure 1 of the *JiNao Report*, which the Defendants argue discloses a hierarchical system wherein low-level "Local JiNao" monitors analyze data and higher-level "Remote Management Applications" analyze the results of the low-level monitors. The Defendants also cite to text from the *JiNao Report* which they characterize as disclosing that "information from lower-level monitors *could be* integrated and correlated at a higher-level monitor for intrusion detection." Joint Invalidity Brief (D.I. No. 299) at 40 (emphasis added).

The Defendants' arguments concerning the alleged "hierarchy" disclosures found in the *JiNao Report* mischaracterize the record surrounding this issue, as well as the *JiNao Report* itself. The hierarchical system purportedly "disclosed" by the *JiNao Report* was, in fact, merely aspirational, as the document itself makes clear:

While it is not within the scope of this project, we expect that the detection/analysis functions implemented in the local subsystem can be extended to a global level and correlate intrusion events among several routers.¹⁹

¹⁹ Ex. F at 3.

The deposition testimony of Frank Jou, the principal investigator of the JiNao project and author of the *JiNao Report*, further proves that the proposed hierarchical analysis capabilities, while objectives of the project, were never attained. In response to questions about the attainment of the goal described in the text cited above, Mr. Jou testified as follows:

Q. Now, while your DARPA project was limited in time and funding, did you create the design such that it could be extended in this hierarchical fashion?

A. I would not say created, because the SNMP network by its nature is to monitor remote system.

Q. Um-hmm.

A. And be able to reflect a healthy -- the healthy -- the status of the network, you know, it's healthy, whether it's healthy or it's, you know, under stress. That was the intent of the SNMP framework. And our thinking at that point in time was to take advantage of this SNMP by the fact that it's able to monitor several systems in a distributive fashion. And you know, the challenge at that point was how do you correlate. I think that was the main technical challenge at that point in time in terms of how do you collect -- collect of the local detection result was not an issue. The issue was how do you come up with the intelligence, how do you correlate all the relevant information and be able to, you know, derive a certain logical or reasonable conclusion, and able to, based upon this result, take action accordingly. I think that was the challenge, and the -- you know, we did look into that aspect. But however at that point we did not have a very promising, you know, development at that time. At the conclusion of the project. So that was, you know, the open question at that point.²⁰

Mr. Jou viewed this "open question," which persisted to the conclusion of the JiNao project in 1999, as a serious technological challenge, and expressed doubt that the goal of hierarchical analysis could have been achieved even with more time and resources:

Q. Had you had more time and money, would you have taken that natural extension step to a more global system?

A. Definitely that was in our intent. But you know, again I should say this was a research project. There was no guarantee, you know, we would be able to bear any fruit even though if the time or resource is allowed at that point in time.²¹

²⁰ Ex. G at 172:1-173:11.

²¹ Ex. G at 170:18-171:2.

If the author of the JiNao reference did not believe his system as described therein incorporated a hierarchical monitor capable of automatically receiving and integrating reports of suspicious activity from other monitors, and potentially might never have such capability, it is hard to imagine how the reference could have taught the system recited in the claims to one of ordinary skill in the art.

Aside from pointing to the referenced figure and text from the *JiNao Report* cited above, which fails to come close to the level of proof they need, the Defendants provide no evidence showing that the *JiNao Report* enables a system having one or more “hierarchical monitors” capable of “automatically receiving and integrating reports of suspicious activity” as recited in the asserted independent claims.²² Presumably, the Defendants rely on the opinion of Mr. Heberlein and the vague “claim chart” attached to their brief. However, the Defendants’ evidence is directly contradicted by the deposition testimony of Mr. Jou, cited above, and the expert testimony of Dr. Kesidis.²³ Summary judgment is appropriate only when there is no genuine issue as to any material fact. FED. R. CIV. P. 56(c); *Celotex*, 477 U.S. at 322. Accordingly, at the very least, questions of material fact exist as to whether the *JiNao Report* teaches and enables the claimed hierarchical monitor automatically receiving and integrating reports of suspicious activity of the ’203, ’615 and ’212 patents, and the Defendants’ motion for summary judgment must be denied.²⁴

Although the Defendants do not address the issue in their discussion of the ’203, ’615, and ’212 patents, their arguments concerning anticipation of the asserted hierarchical claims of those patents must fail for the additional reason that the JiNao Report does not disclose a system that detects suspicious activity by an analysis of network traffic data, *i.e.* packets. Instead, as explained in more detail below, the JiNao

²² Defendants entire discussion on this issue amounts to less than one page in their brief.

²³ Ex. B ¶¶ 100-106.

²⁴ Although again not mentioned by Defendants, dependent claims of the ’338 patent, including claims 13 and 14, require hierarchical analysis and, as such, also are not anticipated by JiNao.

system analyzes audit logs generated by the router to which it is related. Audit logs are not packets and therefore analysis of intrusions based on audit logs is not what is claimed in the patents, which refer specifically to analysis of network traffic data. [Ex. B ¶¶ 101-103; Kesidis Decl. ¶ 28]. For this additional reason, the Defendants' request for summary judgment as to the hierarchy claims must be denied.

2. The *JiNao Report* does not anticipate the '338 claims

The JiNao system operates in a fundamentally different manner from the inventions described and claimed in the '338 patent. Rather than basing its analysis on network traffic data, the JiNao system operated on audit logs generated by a router and, accordingly, was much more akin to the "host-based" systems of the prior art than the network intrusion detection system of the patent. Although JiNao did apply statistical methods and generated long-term and short-term statistical profiles, the data that formed the basis of these profiles was audit data. As such, JiNao did not build statistical profiles "from at least one measure of the network packets" as required by the independent claims of the '338 patent. [See Kesidis Rebuttal Report at ¶ 101-103] Accordingly, JiNao does not anticipate and the Defendants' motion must be denied.

Despite these fundamental differences, the Defendants argue that the *JiNao Report* anticipates the claims of the '338 patent. To support this contention, the Defendants cite various portions of the deposition testimony of Dr. Kesidis, which they characterize as concessions that the system described in the *JiNao Report* satisfies all of the elements of claim 1 of the '338 patent. In fact, this is an inaccurate and self-serving portrayal of portions Dr. Kesidis' testimony, taken out of context. Importantly, the Defendants rely almost exclusively on Dr. Kesidis' excerpted testimony and ignore the disclosure of the *JiNao Report* itself. The text of the *JiNao Report* refutes the Defendants' arguments, and their motion for summary judgment should be denied on that basis.

As the Defendants explain in their discussion of the history of the intrusion detection field, early systems focused on the analysis of audit logs.²⁵ JiNao was such a system. The Defendants' anticipation arguments suggest that the analysis component of JiNao, like the patents-in-suit, directly received data packets as they moved through a network and built measures from those packets. That is simply not the case. The *JiNao Report* unequivocally discloses a system that analyzes audit logs compiled by routers, and not data packets "received" by the router or the JiNao system itself.

The section of the *JiNao Report* entitled "Measures" makes clear that JiNao analyzes audit data:

We would classified [sic] the Ji-Nao measures into two groups: activity intensity and *audit record* distribution measures. . . . These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of *audit data* generated. The *audit record* distribution measure determines whether, for recently observed activity (say, the last few hundred *audit records* received), the types of actions being generated across neighbors are normal.²⁶

The section of the *Report* entitled "Half-life" continues:

The specification of a half-life determine the number of *audit records* or days of *audit record activity* that constitute short-term and long-term behavior.²⁷

The *Report* further clarifies that the aforementioned "activity intensity" measure — "Q" in the language of the *Report* — is also based on audit data:

Q is the sum of *audit record activity* over the entire past activities, exponentially weighted so that the more current activity has a greater impact on the sum.²⁸

Numerous other disclosures make clear that the analysis of the JiNao system is not based on network packets, but instead is based on audit logs—some of which may be generated

²⁵ Joint Invalidity Brief (D.I. No. 299) at 6-7.

²⁶ Ex. F at 19.

²⁷ *Id.*

²⁸ *Id.* at 20.

in “response” to the receipt of certain kinds of packets from the network.²⁹ This is a critical distinction between the JiNao system and the patents-in-suit. The *JiNao Report* does not disclose direct receipt of network data packets or building profiles from measures of these packets, and therefore, it does not anticipate the patents-in-suit.

Dr. Kesidis outlined in his Rebuttal Report on Validity (Ex. B ¶¶ 101-103) that JiNao analyzed audit log data. Thus, his opinion is fully consistent with the actual disclosure of the JiNao Report, and his deposition testimony was not to the contrary. When questioned on the relevance of JiNao to the patents-in-suit, Dr. Kesidis reiterated his view that, although the statistical algorithms used in the JiNao system and the patents-in-suit are superficially similar (which is not surprising, given that both derived from earlier SRI work), the JiNao system analyzes audit logs, while the patents-in-suit analyze network packets directly:

A. The context is -- that statement I made is simply pointing out that you're looking in the one case at host-based audit logs and in the other case at network packets whizzing by on the wire. So any statistical algorithms, statistical algorithms, will have gross features in common but, depending on the time series and the nature of the data you're examining, will necessarily be quite different.³⁰

In subsequent questioning about JiNao's use of network packets, Dr. Kesidis attempted to answer as precisely as possible, stating that JiNao *reacts* to network packets.

Q. Did the JiNao system look at network packets?

* * *

A. Did it look at network packets? It clearly reacted to network packets, so it definitely -- it definitely reacted to them.

Q. What do you mean, it reacted to network packets?

A. Well, JiNao is primarily about detection of anomalies that pertain to the routing protocol, in this case, OSPF, the interior gateway protocol of OSPF. And this protocol -- a protocol is a program that's run by different machines, and they message each other as part of the execution of the program. And in the Internet, those messages are carried in Internet

²⁹ See, e.g., Section 4.1.3.1.3, entitled “Computing the Q statistics for the audit record distribution measures.” *Id.* at 21

³⁰ Ex. H at 43:18-25.

packets. So in that sense, the messaging of the protocol uses IP, and JiNao is about examining the operation of OSPF in a router. And that operation reacts to route updates and other kinds of OSPF-related messages that are delivered by packets. So I can't say that it doesn't react to packets, therefore.³¹

Dr. Kesidis' statement that JiNao *reacts* to network packets accurately reflects the fact that JiNao analyzed information that had been generated by a router in reaction to certain types of packets from the network, *i.e.* the router audit logs, not that JiNao directly analyzed network packets. Dr. Kesidis made this distinction even more clearly in his response to subsequent questioning:

Q. And how did JiNao not look at packets flowing on the wire?

A. Well, in a couple of ways. The first is that it's examining only those packets that are in receipt by the router that it's trying to protect and on which it's trying to conduct intrusion detection. And only those packets that, in the case of the example in the paper, are germane to OSPF. And it's certainly reacting to elements in the payload to a level of detail that's simply out of the scope of these patents and would simply not be feasible. I went through the noninfringement story with regards -- sorry, the validity story with regard to JiNao in my report, and I could look through it.³²

The Defendants characterize the following statement as a concession by Dr. Kesidis that the JiNao Report discloses "receiving network packets":

Q. Let me ask you, just going to the next element on the '338 patent where it says, "receiving network packets handled by a network entity." I believe you said a router is a network entity. Am I right?

A. Sure.

Q. And did JiNao receive packets handled by a router?

* * *

A: In that context, sure. It reacted to packets that are -- certain packets that are received by the router. So in the sense that it reacts to those packets, it receives them.³³

³¹ Ex. H at 44:5-45:4.

³² Ex. H at 49:24-50:9.

³³ Ex. H at 50:16-51:4.

Although Dr. Kesidis states that JiNao “receives” network packets, it is clear from the context of his previous statements and his previous use of the terms “reacts” and “receives” that his meaning is not that JiNao receives network packets directly, but that it reacts to network packets received and logged by a router. Again, testimony occurring after the portion cited by the Defendants makes this clear. When asked again whether JiNao receives packets, Dr. Kesidis again maintained that JiNao receives network packets only in the qualified sense that it reacts to packets received by a router:

Q. Does it meet the first element, receiving network packets handled by a network entity?

* * *

A. The router receives the packets, strictly speaking. So JiNao is a mechanism sitting in a router that reacts to the receipt of those packets. So I would say qualifying it, yeah, you’re right.

Q. So does JiNao meet that first element or not?

A. I -- I mean, again, it’s not receiving the network packet. It’s reacting to certain attributes of it that are -- the packets already in receipt by the router or the line card on which JiNao is functioning.³⁴

The Defendants have exploited Dr. Kesidis’ use of the terms “react” and “receive” by extracting sound bites from the totality of his testimony. Restored to their proper context, however, it is clear that Dr. Kesidis’ statements are consistent with the position stated in his Rebuttal Report on Invalidity, that the JiNao system does not receive network packets, but instead analyzes router audit logs. That distinction precludes summary judgment here.

At minimum, a factual question exists as to whether the JiNao Report describes a system that analyzes network packets, as the Defendants contend, or instead analyzes audit logs created in response to receipt of certain packets, as SRI and Dr. Kesidis contend. The existence of this factual dispute precludes the grant of summary judgment here, and the Defendants’ motion must be denied.

E. The Defendants' Failure to Address Secondary Considerations of Nonobviousness Precludes Any Summary Judgment of Invalidity Under § 103

When considering a motion for summary judgment, all evidence must be viewed in a light most favorable to the non-moving party and all inferences must be drawn in favor of the nonmoving party. *Matsushita*, 475 U.S. at 587. In accordance with Federal Circuit case law, "secondary considerations, when present, must be considered in determining obviousness." *Ruiz*, 234 F.3d at 667. Thus, when summary judgment of obviousness is sought, the evidence that must be viewed in a light most favorable to the non-movant includes any evidence of secondary considerations of non-obviousness. *Rockwell*, 147 F.3d at 1366. The existence of material issues of fact concerning such secondary considerations will preclude summary judgment of obviousness. *Id.*; *Monarch*, 139 F.3d at 886.

SRI has presented substantial evidence of secondary considerations of non-obviousness.³⁵ Dr. Kesidis, in his Rebuttal Report on Validity, identifies for example: the success of EMERALD in competing with other research proposals for DARPA funding, coupled with the willingness of DARPA to fund the EMERALD project; respect of others in the field, as exemplified by numerous EMERALD publications in

³⁴ Ex. H at 55:6-22.

³⁵ Courts have considered secondary considerations of non-obvious other than those enumerated in *Graham*, 383 U.S. at 17. See, e.g., *Scimed Life Systems, Inc. v. Johnson & Johnson*, 225 F.Supp.2d 422, 440 (D. Del. 2002) ("In determining whether an invention is non-obvious, there are at least nine objective factors, *i.e.*, "secondary considerations" that may be considered: (1) a long-felt and unmet need in the art for the invention; (2) failure of others to achieve the results of the invention; (3) commercial success of the invention; (4) copying of the invention by others in the field; (5) whether the invention was contrary to accepted wisdom of the prior art; (6) expression of disbelief or skepticism by those skilled in the art upon learning of the invention; (7) unexpected results; (8) praise of the invention by those in the field; and (9) independent invention by others.").

competitive peer-reviewed journals; recognition by commercial clients, and by DARPA and other government entities; long-felt but unresolved need for the EMERALD technology; and evidence of commercial success of infringing products sold by the Defendants that embody and infringe the claimed inventions. [Ex. B ¶¶ 151-159].

The Defendants have ignored all of these secondary considerations. Because SRI, as the non-moving party, is entitled to have all evidence and all inferences drawn in its favor, the Defendants are not entitled to summary judgment of invalidity of any claim of the patents-in-suit on obviousness grounds.

IV. CONCLUSION

For all of the foregoing reasons, and for the reasons stated in SRI's briefing on its own motions for summary judgment that the *Live Traffic* article is not a section 102(b) prior art publication and for partial summary judgment of no anticipation by the EMERALD 1997 publication, SRI respectfully requests that the Defendants' motion for summary judgment of invalidity of the SRI patents-in-suit be denied and that SRI's motions for summary judgment of no anticipation by the *Live Traffic* article and the EMERALD 1997 publication be granted.

Dated: June 30, 2006

FISH & RICHARDSON P.C.

By: 

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
FISH & RICHARDSON P.C.
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
FISH & RICHARDSON P.C.
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

50355776.doc

CERTIFICATE OF SERVICE

I hereby certify that on July 10, 2006, I electronically filed the **REDACTED – SRI INTERNATIONAL, INC.’S RESPONSE TO DEFENDANTS’ JOINT MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 AND 103** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-
Counterclaimant
Internet Security Systems, Inc., a
Delaware corporation, and Internet
Security Systems, Inc., a Georgia
corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-
Counterclaimant
Symantec Corporation

/s/ John F. Horvath
John F. Horvath